FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 June 2016

Alert Number
MC-000075-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately**.

Email:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP: GREEN:** The information in this product is useful for the awareness off all participating organizations within their sector or community, but not via publicly accessible channels.

Unpatched Ubiquiti Network Devices Subject to Virus Attack Resulting in Denial of Service

Summary

Self-propagating malware has infected thousands of devices from wireless equipment vendor Ubiquiti Networks running outdated airMAX, TOUGHSwitch, and airGateway firmware. Ubiquiti identified the vulnerability and released a patch in July 2015. We have seen an active outbreak of this virus recently on unpatched Ubiquiti network devices. The recent availability of active exploits and the ease with which they propagate means administrators should consider patching vulnerable systems a high priority. The malware scans for and distributes itself to other vulnerable systems, causing mass infections from the virus.

Technical Details

The virus affects the following Ubiquiti devices. For protection against the virus, devices should be running at least the firmware versions noted. All versions of firmware prior to those listed are vulnerable:

- airMAX M (5.5.11 XM/TI, 5.5.10u2 XM, 5.6.2+ XM/XW/TI)
- airMAX AC (7.1.3+)
- ToughSwitch (1.3.2)
- airGateway (1.1.5+)
- airFiber (2.2.1+ AF24/AF24HD, 3.0.2.1+ AF5x)

The virus gains access through the device's hyper text transfer protocol (HTTP) and the secured HTTPS variant and denies access to the device. If the

firmware is out of date, it leaves the HTTP and HTTPS interfaces exposed to the Internet, and the virus can access the device. The malware scans for subnets and will distribute itself to other Ubiquiti systems it identifies.

Recommended Steps for Initial Mitigation

Ubiquiti provided update, mitigation, and removal recommendations for this vulnerability in its community forum at http://community.ubnt.com/t5/airMAX-General-Discussion/Malware-Removal-Tool-05-15-2016/m-p/1564953.

Reporting Notice

The FBI encourages recipients who identify the use of tool(s) or techniques discussed in this document to report information to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by e-mail at CyWatch@ic.fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:
https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.